

METHOD AND APPARATUS FOR DEFENDING AGAINST SYN PACKET BANDWIDTH ATTACKS ON TCP SERVERS

Abstract of the Disclosure

- 5 A SYN packet bandwidth Distributed Denial-of-Service (DDoS) attack is defended against by intercepting and identifying SYN packets in a “DDoS gateway” advantageously positioned at the edge of the network to be protected (*e.g.*, one hop upstream from the protected link), and by queuing these intercepted SYN packets in a separate queue from other TCP packet queues. Edge per-flow queuing is employed to
- 10 provide isolation among individual TCP connections sharing the link. A fair scheduling algorithm such as round robin scheduling is used to ensure that SYN packets (such as those generated as part of a SYN bandwidth attack) cannot overwhelm the egress link in the presence of other TCP packets.